Flux transfrontières de données, vie privée et groupes d'entreprises

Poullet, Yves

Published in:
Revue Lamy Droit de l'Immatériel

Publication date:
2005

Document Version
le PDF de l'éditeur

La Commission belge de protection de la vie privée émettait le 15 mars 2005 à la demande du ministre de la Justice un avis (1) sur les « *Règles d'entreprises* » visant à légitimer un transfert de données à caractère personnel vers des pays non membres de la Communauté européenne. En l'occurrence, le ministre avait été saisi par une entreprise multinationale dont un siège était localisé en Belgique, des règles d'entreprises visant à assurer de manière uniforme la protection des données des employés dans l'ensemble des sièges du groupe.

Flux transfrontières de données, vie privée et groupes d'entreprises :

À propos d'une opinion récente du Groupe de travail « *Article 29* » sur la protection des données et d'une décision de la Commission belge de protection des données

Par Yves POULLET
Doyen de la Faculté de droit
Directeur du CRID

1. Le 3 juin 2003, le Groupe de travail dit de « *l'article 29* » sur la protection des données a adopté le document de travail : « *Transferts de données personnelles vers des pays tiers : application de l'article 26.2 de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données* » (2).
Le document entend résoudre la question délicate de la circulation des données protégées par la directive n° 95/46/CE au sein de groupes d'entreprises dont la dimension dépasse les frontières de l'Union européenne. La solution originale proposée se justifie par les particularités de la situation des multinationales, qui peuvent difficilement se satisfaire des solutions proposées dans ou sur la base de la directive. Cette solution originale présente une réelle continuité avec les principaux traits des solutions déjà définies ; elle entend accentuer une reconnaissance de la valeur de l'autorégulation, comme mode normatif susceptible d'offrir une protection adéquate des données.

2. Avant d'aborder l'analyse de ces solutions (II), il importe d'en situer le double contexte (I) : celui économique décrit la réalité des flux transfrontières au sein des groupes d'entreprises (A), celui juridique situe les diverses solutions jusqu'alors adoptées et confirme leur inadéquation dans le cas précis (B).

I. – LE DOUBLE CONTEXTE

A. – Le contexte économique : les groupes de sociétés (3)

3. La globalisation des marchés en même temps que les stratégies de regroupement d'entreprises expliquent le développement des groupes d'entreprises et la multiplication des flux au sein de ces groupes. Le phénomène certes n'est pas neuf mais prend une dimension nouvelle ; ainsi, comme le montre le cas soumis à la sagacité de la Commission belge, la mobilité requise des compétences humaines au sein de ces groupes justifie sinon la constitution de bases de données centrales relatives au personnel, au moins des possibilités de transfert de données relatives à ces derniers. Les spécialisations des établissements au sein de ces groupes, la répartition des marchés, exigent le partage d'informations quant aux clients tantôt afin de leur fournir un service global, tantôt afin de leur proposer des services complémentaires. Ainsi, la banque établie en Europe pourra servir de guichet unique pour les services bancaires ou autres offerts par les autres membres du groupe. Ainsi, se partagera-t-on volontiers au sein du groupe des fichiers marketing.
La notion de « *groupes d'entreprises* » est difficile à définir et le « *Groupe 29* » ne s'y risque pas. Sans doute, soulignera-t-on que les relations entre membres du groupe peuvent être plus ou moins distendues, plus ou moins hiérarchisées. Entre, d'une part, la simple entente au sein d'un groupe international conclue entre entreprises autonomes dans leurs directions et stratégies et, d'autre part, la filiale entièrement pilotée par la maison mère, il y a peu de ressemblances et, sans doute, les flux seront tant quantitativement que qualitativement plus importants dans le second cas que dans le premier. Nous reviendrons sur ce point qui n'est pas sans conséquence sur la recevabilité des solutions proposées. >

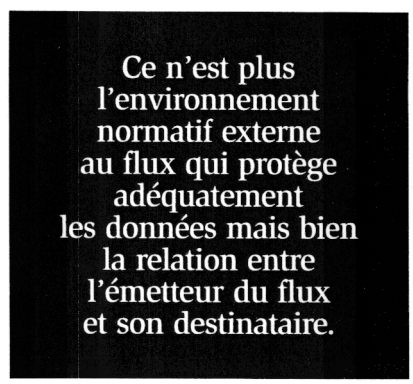
Il va en effet de soi qu'une structure fortement hiérarchisée dispose d'autres moyens de pression et de contrainte pour faire respecter les décisions prises en son sein, et ce, à l'inverse d'une structure plus éclatée sans unité de direction et de stratégie (4). Nous aurons l'occasion de montrer combien cette considération est relevée par le Groupe dit de « *l'article 29* ».

4. Une autre caractéristique du groupe est sa dimension évolutive : le groupe d'entreprises peut s'étendre à de nouveaux territoires (implantation de nouvelles filiales ou succursales, « *joint ventures* » avec des entreprises, etc.) ou, à l'inverse, se restreindre en cas d'abandon ou de ventes d'activités ou de retrait de certains pays. L'existence de configurations géographiquement variables dans le temps crée indiscutablement une difficulté : là où les flux n'étaient envisagés que vers certains pays, des décisions d'investissement ou de délocalisation peuvent amener des implantations nouvelles non prévues au départ. Dès lors, en termes de réglementation de protection des données, il est difficile de prendre en considération la situation existante dans des pays dont la liste n'est point close.

5. À cette variabilité géographique du groupe d'entreprises, s'ajoute celle plus importante des flux intra-groupes, dans la mesure où ceux-ci entendent profiter au maximum de leurs multiples implantations, des réglementations existantes dans les divers pays et des stratégies mouvantes de concertation entre les diverses unités pour modifier, intensifier, rediriger les flux d'informations y compris nominatives entre ces unités. Ainsi, peuvent-elles décider de centraliser les informations relatives au personnel pour accroître la mobilité de celui-ci, pour mener des politiques cohérentes voire uniformes de promotion ou de contrôle des travailleurs. Elles conduiront des stratégies de marketing à direction d'un pays à partir de tel ou tel pays selon les ressources qu'elles peuvent y trouver et les relations avec les fournisseurs hier décentralisées, peuvent demain se trouver centralisées. Bref, la dynamique changeante du groupe influe profondément sur la structure, la quantité et la qualité des flux.
Une dernière considération a trait à l'ancrage européen du groupe d'entreprises. Plus cet ancrage est important, plus la culture réglementaire européenne peut facilement dominer les opérations des autres membres du groupe. On conçoit que pour un groupe dominé de l'extérieur de l'Europe, que ce soit du Japon ou des États-Unis, les principes mêmes de la directive européenne de protection des données à caractère personnel soient difficilement intégrés dans les stratégies décidées à partir de la maison mère. Le faible ancrage des activités d'une multinationale aura une seconde conséquence : les données nominatives collectées en Europe représenteront un faible pourcentage des données traitées par la multinationale et on peut craindre dès lors que les autorités du groupe aient quelque difficulté à justifier de précautions ou garanties liées à la provenance de données minoritaires. On peut craindre que le groupe ne leur oppose que le traitement de l'ensemble des données à des garanties supplémentaires, coûteuses et non exigées légalement pour les données qui constituent le contenu majoritaire des traitements opérés par le groupe.

B. – Le contexte juridique : les flux transfrontières de données et la directive n° 95/46/CE (5)

6. On sait que la directive contient diverses dispositions relatives aux flux : la principale est certes l'article 25 qui affirme le principe de la protection adéquate.
En bref, les flux transfrontières de données à caractère personnel protégés par la directive sont interdits vers des pays tiers sauf à démontrer que l'entreprise, le secteur, le pays offrent une protection adéquate eu égard aux risques spécifiques d'atteinte à la protection des données générées par le flux ou le type de flux en question (6). La protection est offerte ici par l'environnement « *normatif* » externe dans lequel s'opère le flux. La Commission, sur la base de l'article 25.6 de la directive, a ainsi considéré, comme offrant des protections adéquates, divers systèmes législatifs (7) ou auto-réglementaires, comme les « *Safe Harbor Principles* » proposés par le « *Department of Commerce* » des Etats-Unis (8).



L'article 26 énonce quant à lui deux types d'exceptions à cette règle de la protection « *adéquate* ». Le premier type, décliné en 7 cas par le point 1 de l'article, vise des catégories de flux particuliers qui, en raison de leurs caractéristiques (9), présentent une légitimité et une proportionnalité telles que les risques d'atteinte sont limités voire réduits à néant. Le second point de l'article 26 prévoit que l'apport de « *garanties suffisantes de protection de données* » peut être opéré par d'autres modes de protection que ceux prévus à l'alinéa 1 : ce n'est plus l'environnement normatif externe au flux qui protège adéquatement les données mais bien la relation entre l'émetteur du flux et son destinataire. On songe bien évidemment au contrat (10) que ces derniers pourraient conclure entre eux et dont les clauses « *appropriées* » auraient pour but et effet d'offrir des « *garanties suffisantes* », en d'autres termes une protection adéquate (11). C'est dans ce contexte et sur cette base des compétences que lui confie l'article 26.4 que la Commission, avec l'aide du « *Groupe 29* », a par deux fois émis des « *clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers* » (12). L'avis émis par le groupe de par l'article 29 et dont nous discutons le bien-fondé s'inspire de la même philosophie. Les « *garanties suffisantes* » procèdent cette fois des règles d'entreprises contraignantes applicables au sein du groupe d'entreprises.

7. Sans doute s'étonnera-t-on de cette nécessité d'ajouter encore aux options offertes aux entreprises localisées hors d'Europe pour échapper à l'interdiction de principe affirmée par l'article 25. Sans doute, la souplesse européenne (13) démontrée par cette option supplémentaire la met un peu plus à l'abri, si besoin en était, des critiques que les règles de l'OMC pourraient fonder (14). En effet, il peut être difficile de ne pas reconnaître dans cette large palette de moyens laissés par l'application de la directive, une volonté de ne pas appliquer de barrières disproportionnées aux flux transfrontières : chaque entreprise peut trouver une solution appropriée à sa situation dont l'application ne représente pas un obstacle insurmontable.
L'ajout de l'option correspond en effet à cette volonté du « Groupe 29 » de ne pas introduire de discrimination à l'égard des multinationales mal-à-l'aise vis-à-vis des autres options comme il est expliqué maintenant.

8. En effet, la « *protection adéquate* » exigée par l'article 25 nécessite la prise en considération des règles externes à l'en-

treprise, règles en vigueur et respectées dans le pays tiers. Sans doute, ces règles peuvent trouver leur origine dans des sources normatives diverses, qu'elles soient de régulation publique ou privée (autorégulation professionnelle ou autres) voire de normes techniques de sécurité, qu'elles soient générales ou sectorielles, mais elles doivent trouver une effectivité dans un territoire donné. La caractéristique des flux au sein d'une multinationale interdit toute stabilité dans la référence à un territoire, comme nous l'avons montré plus haut (15).

Appliquer les exceptions de l'article 26.1 se heurte également à la réalité de tels flux. Sans doute, le consentement indubitable et les nécessités de l'exécution d'un contrat conclu ou à conclure, hypothèses expressément prévues par l'article 26.1 peuvent justifier des transferts au sein de la multinationale. Ainsi, le membre du personnel peut-il consentir à ce que la donnée le concernant soit transférée vers le siège central ou l'exécution du contrat passé avec lui peut-elle légitimer un tel transfert ? Ceci dit, il est difficile de trouver dans ces exceptions dont l'interprétation doit nécessairement être restrictive le fondement des solutions souples recherchées légitimement au sein des multinationales. Ainsi, la première exception prévue par l'article 26.1 réclame le consentement indubitable au transfert envisagé. Cette précision à la fois dans la modalité d'expression du consentement et dans le flux, objet de ce consentement, ne rencontre pas les besoins d'un groupe qui souhaiterait comme nous l'avons montré pouvoir transférer les données d'un lieu à un autre, et envisager, selon les besoins du terrain, des transferts quantitativement et qualitativement variables.

9. Même objection à propos de l'utilisation de l'article 26.1b) qui légitime le flux transfrontières de données uniquement lorsque ce flux, y compris son caractère transfrontières, est justifié de manière nécessaire, par les finalités contractuelles. Il est difficile pour une multinationale de plaider, au regard de cette exception, la légitimité des transferts faits dans l'intérêt d'une bonne gestion de la multinationale (16). Ainsi, une banque de données centralisée hors Europe des employés de toutes les filiales, banque qui reprendrait la qualification des employés et leur historique au sein de la firme peut difficilement être qualifiée de strictement nécessaire à l'exécution du contrat. Seuls des transferts ponctuels à partir des bases de données localisées sur une base nationale et relatifs à certains employés dont on recherche la mobilité pourraient répondre à cette double exigence de l'exception.

L'inadéquation des solutions contractuelles mentionnées par l'article 26.2 est tout aussi patente (17). Sa mise en œuvre exige, c'est l'essence même de contrat, une parfaite identification non seulement des personnes contractantes mais des flux, objet du contrat. Or précisément, cette double nécessité apparaît difficilement satisfaite là où précisément le groupe d'entreprises entend jouer sur une multilatéralité des destinataires potentiels et l'extensibilité de l'objet des flux entre ces partenaires (18).

> La première exigence à laquelle doit satisfaire l'autorégulation est de traduire de manière précise et détaillée les principes fondamentaux relatifs à la protection des données.

Enfin, les trois options proposées jusqu'ici : la protection adéquate, les exceptions de l'article 26.1 et la solution contractuelle apportant des garanties suffisantes souffrent toutes les trois d'une limitation peu compatible avec les exigences des groupes multinationaux d'entreprises. Elles exigent que les territoires ou destinataires vers lesquels sont autorisés les transferts soient circonscrits et que soient évités les transferts « *ultérieurs* » (« *onward transfers* ») vers d'autres destinataires ou d'autres territoires non couverts par le contrat, l'exception de la protection adéquate. Comme nous l'avons dit (supra n[os] 4 et 5), le groupe d'entreprises est une réalité vivante qui ne peut exclure de tels transferts ultérieurs. Faudra-t-il, chaque fois qu'un nouveau siège de la multinationale est créé et participe aux flux générés au sein du groupe, exiger tantôt la vérification de la protection adéquate y offerte (art. 25.2), tantôt la signature d'un nouveau contrat (art. 26.2) avec le siège européen, tantôt le retour vers la personne concernée pour lui demander son consentement (art. 26.1) ?

10. De telles considérations, si elles justifient la création d'une option supplémentaire, ne doivent pas faire perdre de vue la nécessité d'assurer la continuité des principes de base mis en évidence dès 1998 dans le cadre des réflexions sur la protection adéquate et poursuivis dans la rédaction des clauses contractuelles types. Certes, le mode de réalisation de ces principes tient compte des spécificités de la réalité des groupes d'entreprises mais il s'agit toujours ici comme dans le cadre de la protection adéquate de l'article 25 ou celle contractuelle d'assurer une réelle et effective protection des données à caractère personnel. Il nous importera dès lors dans les développements qui suivent (II) de montrer tout à la fois l'originalité et la continuité des solutions apportées.

II. – LA SOLUTION PROPOSÉE : CONTINUITÉ ET ORIGINALITÉ

11. Le document de travail n° 12 : « *Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données* » constitue, parmi les documents produits par le Groupe dit de l'article 29, la référence lorsqu'il s'agit de s'interroger sur la légalité des flux transfrontières (19).

Ce document est guidé par une approche fonctionnelle que par ailleurs nous avions caractérisée comme suit : cette approche repose sur une série de principes fondamentaux en matière de protection des données, ainsi que sur certaines conditions nécessaires pour garantir leur efficacité. En d'autres termes, deux types de règles sont censés garantir la protection adéquate, selon l'article 25.2, ou suffisante, selon l'article 26.2. Il s'agit des règles de fond relatives à la protection des données et de règles visant à assurer l'effectivité de ces règles dites de fond.

12. La première exigence à laquelle doit satisfaire l'autorégulation est de traduire de manière précise et détaillée les principes fondamentaux relatifs à la protection des données qui peuvent s'énoncer comme suit (20) :

- limitation des transferts à une finalité spécifique ;
- qualité et proportionnalité des données ;
- transparence (des traitements) ;
- sécurité ;
- droits d'accès, de rectification et d'opposition ;
- restrictions aux transferts ultérieurs vers des personnes non couvertes par le champ d'application des règles de protection adéquate.

A. – Les règles de fond et leur application en cas de groupes d'entreprises

13. Ce n'est pas sur ce point que le document de travail n° 74, « *relatif à la protection des données aux règles d'entre-* >

prises contraignantes applicables aux transferts internationaux de données » se montre le plus innovant. Il se contente de les réaffirmer tout en prenant soin d'ajouter que ces principes fixant le contenu substantiel « d*oivent être développés et détaillés dans le cadre de règles d'entreprises contraignantes afin de pouvoir s'adapter de manière pratique et réaliste aux opérations de traitement effectuées par l'organisation dans les pays tiers* (...) ».
L'ajout est important. Il se justifie, note le document de travail, par le fait que l'absence de règles normatives externes explique que certaines entreprises membres du groupe situés dans des pays n'offrant aucune protection adéquate, n'ont dès lors aucune connaissance de la portée de principes comme ceux de la qualité et proportionnalité des données ou de la transparence. Ainsi, il n'est pas évident que les employés d'une filiale brésilienne puissent concevoir que le principe de transparence signifie une obligation d'informer les personnes concernées sur les finalités des traitements poursuivis et de s'interdire toute collecte de données par des méthodes déloyales. Détailler la signification pratique des divers principes a donc une valeur éducative et informative.
Le document de travail suggère une autre justification : la règle de la valeur ajoutée exigée des instruments d'autorégulation (21) signifie que l'autorégulation n'est acceptable que dans la mesure où elle permet de préciser et compléter les principes généraux de la réglementation publique (22).
Au-delà de ces justifications explicite et implicite, on soulignera que cette exigence est parfaitement compréhensible. La norme, dans la mesure où elle concerne des pratiques concrètes au sein d'un groupe d'entreprises, se doit d'être plus détaillée que des normes externes qui doivent s'appliquer à de multiples situations (23). On ajoutera que la valeur obligatoire des « *règles d'entreprise* » dépend bien évidemment de la précision de leur expression, comme il sera dit ci-après.

14. Une règle mérite une attention particulière : celle des « *transferts ultérieurs* ». La règle affirmée par le document de travail n° 12 selon laquelle « *les transferts ultérieurs de données à caractère personnel effectués par le destinataire du transfert initial ne doivent être autorisés que lorsque le deuxième destinataire est également soumis à des règles offrant un niveau de protection adéquat* », reçoit l'interprétation suivante :
- l'adjonction d'une nouvelle entité dans un groupe oblige le groupe, sous peine de voir les flux en direction de cette nouvelle entité considérés comme des transferts ultérieurs soumis à de sévères restrictions :
  - à s'assurer que cette nouvelle entité est effectivement liée par les règles du groupe et qu'elle est en mesure de les respecter,
  - à la tenue d'une liste de filiales mise à jour et la notification de modifications de cette liste une fois par an aux autorités de protection des données ;

La règle de la valeur ajoutée exigée des instruments d'autorégulation signifie que l'autorégulation n'est acceptable que dans la mesure où elle permet de préciser et compléter les principes généraux de la réglementation publique.

- le flux vers une entité soit hors groupe soit membre du groupe, en cas de non-respect des obligations mentionnées ci-avant, oblige à démontrer soit qu'une protection adéquate est offerte, soit la signature d'un contrat avec cette entité apportent une « *garantie suffisante* ».

Dans l'affaire portée à la connaissance de la Commission belge, les garanties prévues en cas de transfert ultérieur des données étaient, d'une part, l'assurance « *par voie contractuelle ou par un autre moyen contraignant* » que le sous-traitant prévoit des mesures de sécurité appropriées et, d'autre part, l'exigence du respect des règles d'entreprise ou la garantie d'un même niveau de protection. La Commission regrette le « *niveau de détail insuffisant* » de tels engagements, en particulier à propos des mesures de sécurité appropriées qui seront à prendre.

15. L'avis n° 74 ajoute à ces réflexions que « *les règles doivent clairement stipuler que lorsqu'une filiale du groupe a des raisons de penser que la législation qui lui est applicable risque de l'empêcher de remplir ses obligations en vertu des règles d'entreprise contraignantes et risque d'avoir un impact négatif sur les garanties fournies, ladite filiale en informera immédiatement le siège européen du groupe* ». L'ajout est important et mérite une explication. Si la loi étrangère applicable à un membre du groupe oblige par exemple ce membre à écouter l'ensemble des communications ou à révéler les membres du personnel du groupe affilié à tel syndicat ou ayant telle ou telle croyance religieuse, cette législation étrangère oblige à un comportement qui pourrait contrevenir aux exigences de la protection adéquate requise par la directive européenne (24).

B. – L'effectivité des règles

1. Rappel des règles

16. Trois conditions sont soulignées pour assurer l'effectivité des règles dont le contenu a été rappelé ci-avant :
- « *assurer un niveau satisfaisant des règles* » : on reconnaît, en général, ajoute le document de travail n° 12, la qualité d'un système à la conscience aiguë qu'ont les responsables du traitement de leurs obligations et les personnes concernées de leur droit. À cet impératif préalable de la connaissance des règles par les deux parties s'ajoutent l'existence de mesures de contrôle internes ou externes de respect des règles et la consécration de sanctions efficaces et dissuasives ;
- « *apporter soutien et assistance aux personnes concernées* » : il s'agit d'abord du souci de protéger la partie faible : la personne concernée contre la partie forte, le responsable du traitement qui peut être le dispensateur de crédit, l'employeur dont on craint les foudres. Ce souci est comparable à celui qui inspire les législations de protection des consommateurs. Au-delà, l'exigence souligne la nécessité pour la personne concernée de pouvoir obtenir une aide face à la complexité et à l'opacité du fonctionnement des systèmes d'information. Un accès rapide, efficace et non coûteux aux services appropriés du responsable des traitements et l'intervention d'une instance indépendante institutionnalisée et ayant compétence pour l'instruction des plaintes répondent à cette seconde exigence ;
- « *fournir des voies de recours appropriées* » suppose la possibilité, en cas de non-respect des règles, d'intervention d'une autorité indépendante publique ou privée compétente pour indemniser la victime ou sanctionner le contrevenant.

17. Dans quelle mesure le document de travail n° 74 applique-t-il ces principes dans le cas particulier des multinationales ? La réponse à cette question nécessite une réflexion préalable. Dans la

mesure où le caractère adéquat de la protection repose non sur des règles externes aux acteurs du flux mais sur des règles propres à ces acteurs, il importe de s'interroger sur le caractère contraignant de telles règles. La question mérite d'autant plus d'être posée qu'il n'est point fait recours au mécanisme du contrat dont chaque ordre juridique reconnaît la valeur obligatoire mais à de simples règles générées par le groupe d'entreprises et auxquelles chaque membre du groupe déclare se soumettre.

On s'interroge donc sur la portée d'un règlement interne à une multinationale. Quelle valeur reconnaître à un document par lequel un groupe régule ses flux internes ? Le phénomène de l'autorégulation définie comme technique selon laquelle des règles de droit ou de comportement sont créées par les personnes auxquelles ces règles sont destinées à s'appliquer (25). À l'inverse des règles professionnelles ou de codes de conduite sectoriels, l'autorégulation n'est pas ici imposée de l'extérieur de l'entreprise ou à son groupe, elle est générée en leur sein sous forme d'une charte, d'un code de conduite, d'une « *Privacy Policy* » du groupe ou d'un règlement édicté par la maison mère (26).

2. Le caractère contraignant des règles du groupe : une double signification

18. Pour le caractère contraignant de telles règles, le document de travail distingue le plan du droit (le caractère juridiquement exécutoire) et le plan pratique pour affirmer tout de suite que si le caractère contraignant doit être apprécié sur les deux plans, le second plan est important dans une configuration transfrontalière où la reconnaissance des droits s'avère difficile et où « *il importe (dès lors) non seulement de veiller à ce que les règles internes soient exécutoires d'un point de vue juridique mais également d'un point de vue pratique* ».

L'étude du CRID (27) à la base de l'adoption du document de travail n° 12 : « *Transferts de données à caractère personnel vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données* », document approuvé le 24 juillet 1998 (28), plaidait en effet pour une prise en considération, à côté des moyens fondés sur le droit et susceptibles d'entraîner condamnation judiciaire, de méthodes de contrainte fondées cette fois non sur le droit, mais la déontologie, la crainte de l'exclusion d'un secteur, ou de représailles médiatiques voire d'un boycott de l'entreprise.

L'existence de tels moyens contraignants d'essence non juridique prend dans le contexte d'un groupe une coloration particulière. Premièrement, ils sont aisés à deviner et à mettre sur pied. Le document de travail n° 74 que nous commentons note : « *À cet égard, divers éléments s'avèrent pertinents, comme l'application de sanctions disciplinaires en cas d'infraction* ».

On sait que l'unité économique que peut représenter un groupe de sociétés ne se conçoit pas sans une structure hiérarchique forte et des moyens de contrôle importants du respect des décisions prises à la tête du groupe (29). La structure interne du groupe donne donc aux décisions d'autoréglementation prises en son sein et au plus haut niveau une force évidente mais, dans le même laps de temps, il faut bien reconnaître que dans le domaine qui est celui de la protection des données, l'intérêt poursuivi n'est pas nécessairement l'intérêt économique du groupe même si la bonne gestion des données nominatives peut contribuer à la bonne image du groupe. En d'autres termes, il n'est pas toujours évident que la règle, le code de conduite ou la *privacy policy* décidés au sein du groupe fassent l'objet d'une attention particulière de la hiérarchie du groupe, s'il n'y a pas menace de contraintes cette fois juridiques, forçant la hiérarchie à utiliser les moyens de pression et de contrainte internes au groupe. Deux autres facteurs atténuent fortement l'efficacité des moyens internes lorsque la multinationale est majoritairement implantée en dehors d'Europe. Le premier souligne la difficulté pour la (ou les) filiale(s) européenne(s) minoritaire(s) au sein du groupe de veiller au respect de règles pas nécessairement mais souvent proprement européennes. Le second constate que les règles internes motivées par les exigences européennes risquent de n'avoir pour champ d'application que les données à caractère personnel provenant d'Europe et d'introduire dès lors dans la gestion des flux et des bases de données une double réglementation : celle applicable à la majorité des données, et dès lors mieux connue, et celle plus exceptionnelle relative aux seules données européennes.

> Le précédent du « *Safe Harbor* » mérite d'être relevé pour bien comprendre la difficulté de l'approche proposée ici.

19. En conclusion, il est difficile de porter un jugement *a priori* et univoque à propos de l'efficacité des moyens de contrainte non juridiques. *A priori*, elle dépendra de la structure plus ou moins hiérarchisée du groupe, de l'autorité au sein du groupe ayant adopté les règles, du poids des entreprises européennes dans le groupe et du champ d'application du règlement non restreint aux seules données « *européennes* ». On ajoutera que la création au sein de la multinationale d'un organe-relais indépendant (30), une sorte de « *détaché à la protection des données* » capable de veiller au respect des exigences légales, représente une garantie complémentaire utile dans la mesure où ce « *détaché* » a une réelle compétence d'enquête et de contrôle, peut rapporter les défaillances constatées aux organes exécutifs centraux du groupe et proposer les corrections nécessaires.

On conçoit dès lors que le « *Groupe 29* » ait exigé explicitement une nature contraignante des règles tant en droit qu'en pratique et souligné le caractère complémentaire de cette double contrainte même si le document souligne le caractère prépondérant de la contrainte non juridique. « *Si la possibilité pour les personnes concernées de faire respecter les règles en recourant à la justice constitue un élément nécessaire pour les raisons qui viennent d'être exposées, le Groupe de travail "Article 29" attache encore plus d'importance à l'application pratique de ces règles par le Groupe dans la mesure où il s'agit là de la finalité de toute approche fondée sur l'autoréglementation* » (31). On ajoute que le document de travail n° 12 à propos de la protection adéquate n'opérait pas une telle distinction et ne se souciait pas dès lors d'affirmer cette complémentarité nécessaire.

20. S'agit-il donc d'une exigence nouvelle ? L'autorégulation externe pourrait-elle se contenter des seules mesures de contrainte non juridiques ? Sans doute, l'adoption d'un code de conduite sectoriel contrôlé par des organes *ad hoc* mis en place par le secteur et objet, en cas de non-respect, de sanctions comme le boycott, la publicité par le secteur auquel appartient le contrevenant, voire l'exclusion du secteur pourrait conduire à prononcer une adéquation de l'autorégulation selon l'article 25.2. En matière de groupes d'entreprises, les mêmes mesures sont soit impensables, soit risquent de ne plus être mises en branle. Cette crainte d'une autorégulation, livrée à ses >

propres méthodes de contrôle et sanctions a déjà été relevée dans la discussion sur le caractère adéquat des « *Safe Harbor* » présentés par le *Department of Commerce* américain et considérés comme offrant une protection adéquate par décision de la Commission européenne le 26 juillet 2000 (32). On sait que l'élément déterminant du système proposé, qui a finalement emporté la décision positive européenne, a été la constatation que l'organisation (signatrice du « *Safe Harbor* ») est soumise aux pouvoirs légaux d'un organisme public (33) habilité à instruire les plaintes et à obtenir des mesures de redressement contre les pratiques déloyales ou frauduleuses ainsi que la réparation des préjudices subis par les personnes concernées, (...) (34).

21. Le précédent du « *Safe Harbor* » mérite d'être relevé pour bien comprendre la difficulté de l'approche proposée ici. Dans le système du « *Safe Harbor* », le caractère juridiquement contraignant du système d'autorégulation est indéniable mais indirect : c'est dans la mesure où la loi américaine réprime les déclarations d'entreprises « *deceiptive or false* » que la personne concernée, victime d'un non-respect par l'entreprise de sa propre déclaration, pourra se plaindre auprès de cette « *juridiction* » particulière. Ce ne sont pas les règles elles-mêmes de protection des données qui sont ainsi protégées mais le fait de les avoir proclamées et de ne pas s'y tenir.
La nature juridiquement contraignante des règles proclamées unilatéralement (35) par un groupe d'entreprises est en dehors de ce système propre aux États-Unis, peu évidente. Comme le note Wéry (36), « *la principale faiblesse de l'autorégulation unilatérale réside (...) dans son caractère unilatéral et donc en théorie non contraignant : créée par la volonté de celui qui accepte de s'y soumettre, la règle peut également être supprimée ou modifiée par déclaration unilatérale de volonté de cette même personne* ». Certes l'auteur se retranche finalement derrière la reconnaissance par le droit belge de l'acte unilatéral pour rassurer le lecteur belge mais sa démonstration est un peu courte dans la mesure où il doit bien reconnaître que la solution même en Belgique est loin d'être pacifique et ne peut être facilement étendue à l'ensemble des droits européens (37).

22. Sans doute, n'est-il point nécessaire de passer par le détour d'une institution aussi controversée que l'acte juridique unilatéral pour affirmer la nature contraignante de règles, *privacy policies* ou autres déclarations (« *statements* »). Il doit être possible de considérer, selon le principe général de droit de la légitime confiance (38), que celui qui affirme sans détour un engagement public précis et circonstancié avec l'intention claire que cette volonté produise des effets de droit est tenu à l'égard des personnes vis-à-vis desquelles il a entendu s'engager. La constatation, premièrement, qu'in casu cet engagement est délivré à une autorité officielle comme l'autorité de protection des données chargée de veiller à

> Portées à la connaissance des personnes concernées, les règles d'entreprises sont une exigence essentielle dans la mesure où cette information permettra le contrôle le plus effectif du respect des règles.

la protection de personnes concernées, le fait que, deuxièmement, comme condition de l'autorisation d'exportation de données et, troisièmement, que cet engagement est l'objet d'une information de ces personnes bénéficiaires de l'engagement plaident indiscutablement pour la reconnaissance d'une valeur juridique de ce type d'engagement. Le simple fait que l'engagement soit contenu dans un document intitulé « *code de conduite* » ou comme simples règles de comportement ne suffit pas en soi à exclure toute portée juridique au contenu précis et clair de l'engagement. La prépondérance du droit sur les autres ordres normatifs ou plutôt le fait que le droit puisse se mêler de donner efficacité à des prescrits moraux ou éthiques s'il l'estime juste et utile (39) conduit à présumer que le Groupe qui proclame dans les conditions prévues par l'avis n° 74 une « *privacy policy* » est soumis au droit et que celui-ci donnera pleine efficacité à des engagements même pris sans référence explicite à la portée juridique de tels engagements (40).
Sans doute ce que nous affirmons ici devrait être l'objet d'analyses plus approfondies (41) et on peut concevoir l'extrême prudence du Groupe dit de l'article 29 lorsqu'il laisse aux groupes d'entreprises le soin de démontrer qu'au regard du droit déclaré applicable ces documents ont une réelle portée juridique (42).

23. Cette première réflexion « *sous réserve d'inventaire* » conduit à reconnaître une portée contraignante aux règles visées par l'avis en question et ce vis-à-vis de leurs principaux bénéficiaires : les personnes concernées. En l'occurrence, ces tiers sont parfaitement déterminables dans la mesure où il est même fait devoir au groupe de les informer de l'existence de ces règles. De ce fait, « *ils doivent pouvoir faire respecter ces règles en introduisant une plainte aussi bien auprès de l'autorité compétente de protection des données qu'auprès du tribunal compétent* (...) » (43).
Reste la question des entreprises qui au sein du groupe sont liées par cet engagement collectif pris par le groupe au nom des membres dont, en cas de non-respect, la filiale européenne est responsable (44). À cet égard, l'avis recommande la prudence : seules les entreprises directement contrôlées et soumises à l'unité de direction du groupe peuvent se sentir tenues du respect de ces règles à l'inverse de sociétés plus périphériques et autonomes (45). Vis-à-vis de ces dernières, l'avis recommande qu'un contrat avec stipulation pour autrui en faveur des personnes concernées soit conclu : « *dans ce cas, la portée des droits liés au statut de tiers bénéficiaire correspondra au moins à celle prévue par la décision 2001/497/CE de la Commission relative aux clauses contractuelles types tant vis-à-vis de l'exportateur de données que de l'importateur de données* » (46). Ainsi, le Groupe de l'article 29 reconnaît clairement la complémentarité des deux types de garanties suffisantes imaginées sur la base de l'article 26.2.
La Commission belge insiste sur l'importance de la reconnaissance claire par les règles d'entreprise d'un droit à la personne concernée. Cette reconnaissance manquait *in casu* dans les règles d'entreprise qui lui étaient soumises.

3. Analyse des trois conditions d'effectivité au cas de la multinationale (47)

a) Assurer un niveau satisfaisant des règles

24. Cette première condition se décompose en différentes sous-conditions : la « *conscientisation* » à la fois des destinataires des règles, les responsables de traitement et des bénéficiaires des règles, les personnes concernées (n° 27) est exigée mais en outre doivent exister des méthodes de contrôle internes ou externes

du respect des règles. Finalement, des sanctions qualifiées « *d'efficaces et dissuasives* » doivent garantir le respect des règles dans la mesure où le responsable craindra les conséquences du non-respect (n° 28).

25. La « *conscientisation* » des responsables, c'est-à-dire des différentes unités du groupe et des personnes au sein de ceux-ci en charge des traitements suppose que le groupe demandeur du bénéfice de l'exception prévue à l'article 26(2) de la directive soit « *à même de prouver que cette politique (de protection des données) est connue, comprise et effectivement appliquée...* » pour les employés, formés en conséquence (48) et disposant de toute l'information pertinente à tout moment, par exemple *via* l'intranet.
Portées à la connaissance des personnes concernées, les règles d'entreprises sont une exigence essentielle dans la mesure où cette information permettra le contrôle le plus effectif du respect des règles ; celui effectué par les personnes directement concernées par le traitement. L'avis du Groupe de l'article 29 réaffirme le principe : « *Les règles d'entreprise juridiquement exécutoires* (49) *doivent être portées à la connaissance des personnes et aisément accessibles par celles-ci* » (50). En d'autres termes, outre les informations dont la fourniture est imposée par les articles 10 ou 11 (51) au responsable du traitement localisé en Europe, l'avis précise que la communication des données à d'autres filiales situées en Europe doit être l'objet d'une information spécifique et surtout que « *les personnes ont facilement accès aux informations relatives aux principaux engagements pris par le groupe, les filiales liées par les règles ainsi qu'aux moyens mis à la disposition des personnes pour vérifier le respect des règles* ».

26. La formule laisse aux responsables le soin de déterminer la voie par laquelle cette information aura lieu. On le conçoit aisément : informer des employés d'une multinationale ne suivra sans doute pas les mêmes canaux qu'une information à donner à des internautes européens entrant *via* un portail localisé en Europe dans des sites multiples dont la gestion de la base de données clientèle est centralisée hors Europe. Cette exigence de transparence est soulignée par la Commission belge. En l'hypothèse, les employés prévoyaient les règles proposées par la multinationale, auraient été informés par la publication des règles sur le site web interne à l'entreprise et par des hyperliens « *accessibles depuis les applications informatiques servant à la collecte et au traitement des données des employés* ». La Commission estime que cette information est encore insuffisante : « *Il est essentiel que les employés soient directement et clairement informés du fait même de la transmission de leurs données à l'extérieur de l'Union européenne* ». Publier les règles est insuffisant, il faut en outre clairement souligner que ces règles couvrent des transmissions hors Europe.

• Le contrôle du respect des règles peut être interne ou externe : « *Les règles, affirme le Groupe de l'article 29, doivent prévoir des audits internes et/ou externes réalisés régulièrement par des contrôleurs agréés qui transmettront un rapport directement au Conseil d'administration de la maison mère du groupe* » (52), dont copie aux autorités de protection des données (53). L'avis va plus loin dans la mesure où il mentionne le devoir de coopération avec les « *autorités* » de protection des données qui peuvent exiger l'intervention d'experts ou intervenir elles-mêmes.
Les règles soumises à l'avis de la Commission belge prévoyaient une procédure d'audit interne « *conduite par une équipe indépendante des autres lignes de gestion de l'entreprise* ». Elles prévoyaient même la coopération avec les autorités de protection des données dans le cadre d'investigations demandées par ces autorités. Curieusement, la Commission (54) se dit non satisfaite : « *Les règles prévoient que les autorités exportatrices et importatrices coopéreront pour répondre aux investigations ou demandes d'informations des autorités de contrôle. Cette notion est néanmoins distincte de celle d'audit, qui vise des contrôles à caractère plus systématique et structuré* ».

> La communication des données à d'autres filiales situées en Europe doit être l'objet d'une information spécifique.

Nous reviendrons sur ce point à propos de la seconde condition d'effectivité.

• Les sanctions en cas de non-respect doivent être efficaces et dissuasives, c'est-à-dire non purement correctives (55). L'avis est peu disert à ce propos si ce n'est sur un point. Le non-respect du devoir de coopération avec les autorités de protection des données ou le non-suivi de conseils donnés par ces autorités suite à un audit réalisé par ces dernières ou par des auditeurs internes ou externes et portés à la connaissance des autorités entraîne diverses mesures : la publication des conseils de l'autorité de protection voire la suppression ou le retrait de l'autorisation octroyée par l'autorité compétente en matière de flux transfrontières (56). Il est clair que d'autres sanctions internes au groupe pourraient être prévues. Sur base d'un rapport défavorable, les autorités responsables au sein du groupe, le Conseil d'Administration de la maison mère pourraient interdire la continuation de flux voire interdire le stockage de données chez certains membres du groupe. Des mesures disciplinaires pourraient être prononcées vis-à-vis des personnes en charge de traitements jugés non conformes aux règles d'entreprise. Le silence du Groupe de l'article 29 sur de telles mesures pourrait se comprendre comme un certain scepticisme du Groupe vis-à-vis de mesures dont le déclenchement est peu évident s'il contredit l'intérêt économique du groupe et si le poids de l'ancrage européen du groupe est peu significatif. Ce silence contraste avec l'intérêt que le Groupe dit de l'article 29 avait marqué dans son avis n° 12 à propos du « *niveau satisfaisant de respect des règles* » où étaient évoquées les sanctions disciplinaires, les mesures d'exclusion voire de boycott (57).

b) Fournir une assistance et une aide aux personnes concernées

27. Les groupes se doteront « *d'un système de gestion des plaintes individuelles au sein d'un département clairement identifié* ». Les personnes en charge de ce système jouiront d'un degré « *approprié* » d'indépendance. Tels sont les principes affirmés par l'avis mais on conçoit l'insuffisance de règles aussi minimales là où l'avis n° 12 affirmait qu': « *une exigence essentielle à laquelle doit répondre un système de protection des données approprié et efficace est qu'une personne physique confrontée à un problème touchant aux données personnelles la concernant ne soit pas laissée à elle-même mais puisse bénéficier d'un soutien institutionnel pour la solution de ses problèmes* » et surtout « *mettait en garde contre des instances appartenant à la profession ou au secteur concerné, considérées comme insuffisamment neutres dans la mesure où ces instances partagent des intérêts communs avec le responsable mis en cause* » (58). *A fortiori*, aura-t-on quelque >

difficulté à considérer qu'un département du groupe même autonome dans sa gestion pourrait être neutre vis-à-vis des intérêts du groupe dont il relève. On conçoit dès lors que l'assistance et l'aide doivent provenir de l'extérieur du groupe.
L'avis n° 74 répond à cette inquiétude dans la mesure où il désigne cette instance externe neutre : l'autorité de protection des données dont relève le membre du groupe sis dans l'Union européenne (59). La solution étonne par son caractère radical dans la mesure où elle écarte toute solution « *autoréglementaire* ». Ainsi on aurait pu imaginer que l'assistance soit le fait de sociétés ou d'associations de libertés choisies par le groupe, (...) à la limite sur une liste agréée par le Groupe dit de l'article 29. Ce refus peut s'expliquer par la crainte à la fois des responsables de traitement de se trouver confrontés à des associations peu contrôlées et contrôlables ayant peu le souci du secret professionnel en particulier, mais également des autorités de protection des données peu confiantes dans l'efficacité du soutien que pourraient apporter ces instances aux personnes concernées, de leur absence de moyens réels d'investigation et finalement du manque de moyens de sanctions en leur possession. On note, autre requis de l'opinion n° 12 du Groupe de travail dit de l'article 29, que l'accès aux autorités de protection des données est sans doute plus aisé que vis-à-vis d'autorités prévues peu connues, souvent situées en terre étrangère et peu au courant des règles européennes.

28. Si ces explications convainquent, on ne peut que noter que les solutions ici retenues ne reprennent pas la solution des « *Alternative Dispute Resolution Mechanisms* » (ADR) prônées par les « *Safe Harbor Principles* », et dont l'action est décrite en particulier par le FAQ n° 11. On souligne que selon les « *Safe Harbor Principles* », la coopération avec les autorités de protection des données était mise sur le même pied que la désignation de ces « *ADR* ». Quelques doutes avaient été émis à propos de cette équivalence et de « *l'effectivité du support de ces ADR aux personnes concernées* ». Ainsi, nous concluions (60) : « *L'exigence européenne prévue par le Groupe dit de l'article 29 de trouver auprès de cet organisme "support et assistance" n'est pas reprise.* Certes, l'accès doit être, selon les « *Safe Harbor* » « *aisé* » et « *à un coût raisonnable* » mais ne fallait-il pas prévoir – surtout vis-à-vis d'une personne située en pays lointain – que l'organisme puisse investiguer d'initiative sur simple plainte et non être comme le conçoit le système américain, uniquement un lieu de résolution des litiges, ce qui exige que la personne concernée développe elle-même ses griefs et arguments (...). Enfin des doutes peuvent être élevés sur l'effectivité de certaines sanctions. Que se passe-t-il si l'organisme incriminé refuse de modifier ses pratiques ou de dédommager les victimes de ses agissements ?

29. Faut-il voir dans la suppression du choix entre deux modes d'assurer le soutien : celui offert par les ADR et celui né du recours auprès des autorités européennes de protection des données, un recul de l'autoréglementation ou une méfiance vis-à-vis de celle-ci (61) ? Il est clair que si la solution peut apparaître rassurante en théorie, du moins aux défenseurs de la vie privée, la pratique risque de révéler rapidement l'absence de moyens des autorités de protection des données d'accomplir la tâche de support et d'assistance aux personnes concernées. Quoi qu'il en soit, des « *Safe Harbor* » à l'avis n° 74, il semble bien que le Groupe dit de l'article 29 fasse jouer un rôle de plus en plus essentiel aux autorités de protection des données tout en reconnaissant les limites de leurs interventions, ce qui justifie la nécessité que les règles d'entreprise prévoient explicitement le droit de la personne concernée de saisir la justice de son propre pays (62).

Il semble bien que le Groupe dit de l'article 29 fasse jouer un rôle de plus en plus essentiel aux autorités de protection des données tout en reconnaissant les limites de leurs interventions.

c) Offrir des voies de recours appropriées

30. La condition traitée ici renvoie bien évidemment à l'analyse déjà faite du caractère contraignant des règles et du droit des personnes concernées à se prévaloir de ces règles. Il importe qu'une voie de recours devant les juridictions de leur propre pays existe pour ces dernières qui leur permette non seulement la correction des opérations passées et non conformes aux règles mais également une indemnisation des dommages financiers et moraux (ce que le système juridique anglo-saxon qualifie de « *distress* ») des conséquences de ce non-respect.
L'avis n° 74 énonce en ce sens que « *les règles stipuleront que les personnes concernées bénéficieront des droits en matière de réparation et de responsabilité visés aux articles 22 et 23 de la directive* (63) *dans les mêmes conditions et dans la même mesure que si le traitement effectué relevait du champ d'application de la directive relative à la protection des données* (...) ». L'avis ajoute quelques précisions qui alourdissent le caractère contraignant de la règle : le siège européen ou la filiale européenne responsables par délégation de la protection des données « *devraient* » accepter d'une part d'endosser la responsabilité et de prendre les mesures nécessaires pour réparer les actes commis par les autres filiales du groupe hors Europe et d'autre part d'être poursuivis judiciairement dans l'Union européenne (64). Cette solution de la responsabilité conjointe de l'établissement européen et de l'établissement hors Europe fautif avait déjà été imposée dans le cadre des clauses contractuelles types : « *L'exportateur et l'importateur de données conviennent d'être solidairement responsables des dommages subis par les personnes concernées résultant d'une violation (des obligations contractuelles)* ». Il s'agit là comme ici de faciliter le recours de la personne concernée en mettant à charge de l'établissement européen la responsabilité de l'ensemble des agissements du groupe. À lui de démontrer que la violation incriminée n'est pas le fait d'un membre du groupe. On ajoute que le groupe par ces règles doit reconnaître le droit des personnes concernées d'intenter une action contre le groupe et ce devant la juridiction soit de l'établissement européen à l'origine du transfert, soit de l'établissement responsable de la protection des données.

31. Le souci manifesté par le Groupe dit de l'article 29 à la fois d'une responsabilité de la filiale européenne et de recours devant les juridictions européennes est rappelé par la Commission belge dans le cas qui lui était soumis. Les règles d'entreprise qui étaient proposées à son examen prévoyaient la possibilité pour l'employé d'introduire une demande de dommages et intérêts auprès de l'entité suspectée de violation à son endroit des prescrits de protection des données. La Commission souligne les lacunes de telles clauses.

32. On s'étonnera à nouveau de la manière dont le Groupe dit de l'article 29 restreint les choix des multinationales

quant au choix de l'instance en charge de résoudre les litiges. L'avis n° 12, de même que les décisions sur les contrats types, n'excluaient pas, bien au contraire, l'intervention d'arbitres voire d'organes de médiation et on sait combien les « *Safe Harbor Principles* » avaient fait usage de cette liberté en prévoyant simplement l'obligation pour les sociétés américaines qui désiraient bénéficier des avantages de la protection adéquate de choisir un organe de régulation des litiges privés, un « *ADR* ». Les clauses contractuelles types allaient dans le même sens : l'importateur pouvait convenir qu'en cas de litige, soit une médiation conduite par une personne indépendante ou par l'autorité de protection des données serait menée, soit le tribunal de l'exportateur européen serait saisi, soit enfin un arbitrage serait conclu.

Comment expliquer cette restriction voulue par le Groupe dit de l'article 29 à propos des modes de résolution des litiges en cas de flux à l'intérieur d'une multinationale si ce n'est par une crainte que les autres modes de résolution ne soient pas à suffisance effectifs dans la mesure où pèsent de lourdes incertitudes sur le caractère contraignant au plan juridique des règles émises et que la multinationale puissante ne choisisse un mode de résolution devant un « *ADR* » peu au courant du contenu et surtout de la signification des règles de protection des données ?

CONCLUSION

33. L'avis n° 74 complète la panoplie des modes d'intervention de la « *protection adéquate* » requise par la directive pour assurer dans un contexte international la protection des données à caractère personnel.

Le fait-il adéquatement ?

Premièrement, il est patent que les autres modes de protection dits adéquats répondaient mal aux spécificités des flux existant à l'intérieur d'un groupe d'entreprises.

Deuxièmement, l'avis ne s'écarte pas d'un certain nombre d'acquis des réflexions menées jusqu'ici : ainsi l'avis n° 74 se situe dans la droite ligne des réflexions menées depuis 1998 à propos de la protection adéquate. Les exigences relatives tant au contenu des règles à adopter par la multinationale qu'à leur effectivité sont directement déduites de l'avis n° 12 relatif au concept de protection adéquate et les clauses contractuelles types décidées par la Commission sur la base de l'article 26.4 ont inspiré, outre le souci que les règles d'entreprise créent un droit vis-à-vis des personnes concernées, la nécessité d'une responsabilité de l'entité européenne, membre du groupe.

Troisièmement, l'avis est l'occasion de mettre en évidence la différence entre une autorégulation multilatérale ou sectorielle et celle unilatérale que se fixe un groupe. Sans doute, cette différence justifie-t-elle le malaise ressenti par les auteurs de l'avis vis-à-vis de l'effectivité des règles dites d'entreprise ? Indiscutablement, plus qu'une association sectorielle, la multinationale jouit de moyens de contraindre pratiquement ses membres à respecter les règles qu'elle fixe : la forte hiérarchie et les structures de contrôle qui caractérisent le groupe d'entreprises garantissent en effet ce respect. Encore faut-il que la multinationale entende utiliser ces moyens ! À juste titre, l'avis considère indispensable de doubler les moyens de contrainte juridique y compris à disposition des personnes concernées et offrant des recours juridictionnels en Europe ; l'avis donne un rôle important aux autorités européennes ; enfin, l'avis impose une lourde responsabilité aux membres européens du groupe ou tout au moins à l'un d'entre eux.

Cette prudence, si elle est louable, est-elle « *adéquate* » ? Les autorités de protection des données se retrouvent en première ligne pour assurer la protection des données alors même qu'elles sont débordées et singulièrement mal armées pour faire face à des multinationales puissantes.

Quant à ceux qui voient dans l'avis n° 74 une victoire supplémentaire de l'autorégulation, une analyse un peu sérieuse de l'économie de l'avis témoigne au contraire des limites d'une autorégulation certes plus souple, plus précise dans son contenu, plus imaginative dans des modes de contrôle et des sanctions mais, dans le même temps, cette autorégulation ne voit ses qualités s'épanouir que dans la crainte du recours au juge et de l'intervention du gendarme officiel qu'est la Commission. Bref, l'autorégulation fait place à la co-régulation définie comme un « *effective mix* » d'intervention à la fois des pouvoirs publics et privés ; la complémentarité des moyens mis par l'un et l'autre de ces pouvoirs visant à assurer une meilleure effectivité du principe consacré par la règle légale, en l'occurrence l'exigence d'une protection adéquate. ◆

(1) Avis n° 4/2004 du 15 mars 2004, Rapport du président

(2) C'est en effet l'article 29 de la directive n° 95/46/CE qui crée cet organe consultatif indépendant, composé de représentants des différentes autorités de contrôle nationales. Le lecteur consultera les résultats des travaux du Groupe de l'article 29 sur le site : <www.europa.eu/int/comm/privacy>. Deux documents émanant du « Groupe de l'article 29 » en date du 14 avril 2005 ne sont pas intégrés dans la présente étude. Le premier (WP107) précise l'autorité de protection des données leader en cas de sièges européens multiples. Le second (WP108) est une check-list des renseignements à obtenir auprès des groupes.

(3) Sur la notion « floue » de « groupe de sociétés », lire notamment Hannoun C., Le droit et les groupes de sociétés, LGDJ, Paris, 1991. *Cf.* la tentative de définition de l'Union européenne : « Le groupe y est défini selon deux traits principaux : l'état de dépendance de la filiale, que peut traduire la participation en capital ou de simples éléments de fait ; et l'unité de direction des sociétés membres du groupe » (Hannoun C. , *op. cit.*, p. 4). Voir également, les remarques de Benoît-Mouy A., Entreprises et phénomène associatif, *in* La coopération entre entreprises, ABJE, Bruylant, Kluwer, 1993, p. 464 qui évoque des notions légales comme « action de concert » et « contrôle conjoint ». L'auteur conclut : (*eod. loco*, p. 465) : « La pratique a précédé la norme juridique, la créativité et l'imagination des juristes ont fait face au vide législatif ou ont permis des constructions originales adaptées aux nécessités économiques ou aux spécificités des situations ». *Cf.* plus récemment l'étude de Wymeersch E., Comment le droit pourrait aborder certains groupes de sociétés ?, Mélanges van Ommeslaghe P., p. 703 et s.

(4) Sur cette diversité des montages et la difficulté de distinguer nettement les hypothèses, lire Coipel M., Lettre de patronage et droit des sociétés, in Les lettres de patronage, Faculté de droit de Namur – Feduci, Namur Paris, 1984, p. 201 et s. : « *Les deux ensembles que constituent, d'une part, les sociétés dominantes/dépendantes et, d'autre part, les groupes de sociétés se recoupent, certes, mais ne se recouvrent pas entièrement. Il se peut qu'un lien de dépendance existe entre deux ou plusieurs sociétés sans qu'il y ait groupe à défaut de direction unique. En effet, il y a lien de dépendance même si la société dominante n'use pas effectivement de son pouvoir alors que la direction unique doit être effective pour qu'il y ait groupe. D'autre part, il se peut qu'une société exerce effectivement une influence dominante sur la conduite des affaires d'une autre société sans que pour autant, les sociétés soient gérées quant à leurs fonctions essentielles, selon des objectifs et des conceptions identiques : la direction unique fait alors défaut* ».

(5) Pour un exposé complet en la matière, le lecteur se référera aux articles suivants : Havelange B. et Lacoste A.-C., Les flux transfrontières de données à caractère personnel en droit européen, JTDE, 2001, p. 240 et s. ; Poullet Y., Louveaux S. & Perez-Asinari M.-V., *Data Protection and Privacy in Global Networks : An European Approach*, *EDI Law Review* 8, 147-196, 2001; Schwartz P.-M., *European Data Protection Law and Restriction on International Data Flows* , 80 *Iowa Law Rev.* 1995, n° 3, p. 473 et s.; Reidenberg J.-R., *E-commerce and Trans-Atlantic Privacy*, 38, *Houston Law Rev.* 2001, n° 3, p. 719 et s.

(6) Sur la notion de protection « adéquate » au sens de l'article 25.2 de la directive, lire Poullet Y., Havelange B. avec la collaboration de Boulanger M.-H. et Lefèbvre A., Élaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel, Rapport final du centre de recherches Informatique et droit élaboré pour la Commission européenne et publié sur le site du CRID <www.crid.ac.be>.

(7) À noter les décisions prises par la Commission à propos de différents systèmes législatifs jugés adéquats :

- *Decision n° 2000/519/EC of 26/7/2000 pursuant to directive n° 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary*, JOCE 25 août 2000, n° L 215, p. 4 ;
- *Decision n° 2000/518/EC of 26/7/2000 pursuant to directive n° 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland*, JOCE 25 août 2000, n° L 215, p. 1 ;
- *Decision n° 2000/520/EC of 26/7/2000 pursuant to directive n° 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related frequently asked questions issued by the US Department of Commerce*, JOCE 25 août 2000, n° L 215, p. 7 ;
- Decision n° 2002/2/EC of 20/12/2001 pursuant to directive n° 95/46/CE of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, JOCE 4 janv. 2002, n° L 2, p. 13.

Cf. également à propos de la protection proposée par la loi récente d'Argentine, l'opinion du Groupe dit de l'article 29 émis le 3 octobre 2002 (W.P. 63) disponible sur le site de la Commission européenne à l'adresse suivante : <www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/>.

(8) *Decision n° 2000/520/EC of 26/7/2000 pursuant to directive n° 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related frequently asked questions issued by the US Department of Commerce*, JOCE 25 août 2000, n° L 215, p. 7.

(9) Sur la nécessité d'une interprétation restrictive des exceptions, lire Havelange B. et. Lacoste A.C, art.cité, p. 246.

(10) Pour un commentaire sur l'apport de solutions contractuelles au problème de la protection des données, lire Longworth E., *Contractual Privacy Solutions, Towards Information Society and Electronic Citizenship, 22nd International Conference on Privacy and personal data Protection*, Venezia, Sept. 2000, 183-203 ; Huet J., *Study on contracts involving the transfer of personal data between parties to Convention CoE 108 and third countries not providing an adequate level of protection, Council of Europe*, janvier 2001, disponible sur le site <www.legal.coe.int/dataprotection>. Pour une analyse critique de ces clauses, lire Wellberry B. et Barcelo R., *European Commission's Model Contractual clauses : Paving the way for International Transfers or a New Hurdle, Privacy and Information Law report*, Vol.1, 7, 2001, p. 9 et s.

(11) « La notion de « garanties suffisantes », au sens de l'article 26, paragraphe 2, renvoie à celle de « protection adéquate » (Groupe de l'article 29, Document de travail, n° 12, Transferts de données vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données, adopté par le Groupe le 24 juillet 1998, disponible sur le site de la Commission européenne : <www.europa.eu.int/comm/internal_market/fr/dataprot/wpdocs/wp12fr.pdf >.

(12) Décision de la Commission n° 2001/497/CE du 15 juin 2001, JOCE 4 juill. 2001, n° L 181, p. 19 à propos des clauses contractuelles relatives à des transferts de données vers des responsables de données établis dans des pays tiers. Décision de la Commission n° 2002/16/CE, 27 déc. 2002, JOCE 10 janv. 2003 à propos des clauses contractuelles types pour le transfert de données vers des sous-traitants établis dans des pays tiers.

(13) Sur ce refus de tout « impérialisme » européen dans les règles mises en place, Poullet Y., Pour une justification des articles 25 et 26 de la directive européenne en matière de protection des données à caractère personnel , *Liber Amicorum Bart de Schutter*, VUB Press, 2003, p. 243 et s.

(14) À propos de l'application des règles de l'OMC au débat sur les règles européennes en matière de flux trans-frontières de données à caractère personnel, Perez-Asinari M.-V., *Is there any Room for Privacy and Data Protection within the WTO Rules?, The Electronic Communications Law Review, Kluwer*, 2003; *The WTO and the Protection of Personal Data. Do EU Measures Fall within GATS Exception ? Which Future for Data Protection within the WTO e-commerce Context ? 18th BILETA Conference : Controlling Information in the Online Environment*, April, 2003, QMW, London, available at: <www.bileta.ac.uk/03papers/perez.html>

(15) *Supra* n° 5.

(16) On notera au passage que si l'article 26.1 reprend *mutatis mutandis* la plupart des fondements de légitimité des traitements prévus par l'article 7, il omet soigneusement le seul qui eût pu être invoqué, à savoir celui de l'article 7f) qui permet de justifier le traitement lorsque l'intérêt légitime du responsable l'emporte sur ceux de la protection de la personne concernée (dans le même sens, les réflexions de Bellamy (*Chief Privacy Officer de Accenture*), *How Accenture created a global approach to data transfers ?, Privacy Laws & Business International Newsletter*, sept. 2002, p. 9).

(17) À ce propos, les réflexions de Rowe H., *Transfers of personal Data to third countries : the role of binding corporate rules*, CL&SR, 19, n° 6, 2003, p. 491 et les réflexions tirées de l'expérience d'*Accenture* développées in Perez M.-V., *How Accenture created a global approach to data transfers, Privacy Laws & Business Int. Newsletter*, Sept. 2002, p. 8 et s. Il est à noter qu' Accenture avait dès 2001, avant même l'adoption par le Groupe dit de l'article 29, proposé une « *Privacy policy* » pour l'ensemble de son groupe et avait basé sa demande sur l'article 26.2. À l'époque, Accenture s'était vu refuser l'autorisation d'exportation des données.

(18) « *The code of practice approach taken by Accenture, said Bellamy (Chief Privacy Officer d'Accenture), can offer a truly seamless, practical and workable solution to suit the global nature of its business where functional boundaries have replaced national boundaries* » (Perez M.-V., article cité, note 16).

(19) La Commission belge se réfère de même à ce document et à d'autres fondés sur le même document, « *cette analyse s'effectue, dit la Commission, en prenant principalement en considération le document de travail ... susmentionné (celui sur les règles d'entreprises contraignantes) mais également de façon plus générale les critères d'adéquation dégagés par le groupe lors de ses différents avis relatifs aux clauses contractuelles types ou aux principes de la sphère de sécurité* ».

(20) Cette liste est reprise du document de travail n° 12 (p. 5 et s) et appliquée aussi bien à l'article 25.2 (protection adéquate) qu'aux garanties suffisantes visées par l'article 26.2 (*cf.* l'application aux contrats, p. 18). Aux éléments minima couverts par la liste reprise dans le texte, le document de travail n° 12 ajoute d'autres principes qui peuvent exister dans des circonstances spéciales (données sensibles, système d'aide à la décision, etc.).

(21) Sur la diversité des instruments d'autorégulation et une discussion de leur valeur, le lecteur se référera à l'ouvrage : Gouvernance de la société de l'information, Cahier du CRID n° 22, Bruylant – PUN, Bruxelles, 2002 [Berleur J., Lazaro C. et Queck R. (éd.)]. Cet ouvrage reprend des annexes et une bibliographie étendue sur le sujet.

(22) Ce principe de la valeur ajoutée est déjà sous-entendu par l'article 27 de la directive n° 95/46/CE qui encourage « l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions prises en application de la présente directive ». Au-delà on notera les réflexions sur la valeur de l'autoréglementation menées par l'*E-confidence Online Forum* mis en place le 30 mars 2000 par la DG SANCO et chargé de créer un consensus à propos de mécanismes capables de créer la confiance des consommateurs à propos des opérations de commerce électronique (travaux disponibles à l'adresse suivante : <www.dsa-isis.jrc.it/ECF/index.htm>. À propos de ce principe de l'« *added value* », lire nos réflexions *in* Les diverses techniques de réglementation de l'Internet : l'autorégulation et le rôle du droit étatique, Ubiquité, Juin 2000, p. 55 et s. Les instances européennes insistent dans plusieurs documents sur le fait que l'autorégulation doit compléter la réglementation des États membres qui doit se contenter de fixer les standards sans entrer dans le détail. Le principe de la valeur ajoutée est clairement affirmé par le E-confidence créé par la SG SANCO et chargé de créer un consensus à propos de mécanismes capables de créer la confiance des consommateurs à propos des opérations de commerce électronique (travaux disponibles à l'adresse suivante : <www.confidence.jrc.it/default/htm>).

(23) La même remarque vaut pour la solution contractuelle : la clause contractuelle type 2 « Détails du transfert » stipule : « Les détails du transfert, et en particulier les catégories de données à caractère personnel et les finalités pour lesquelles elles sont transférées, sont spécifiés .... ».

(24) .... À moins de pouvoir considérer que cette mesure est nécessaire au sein d'une société démocratique pour préserver des intérêts publics ou privés essentiels au sens de l'article 8 de la Convention européenne et repris par l'article 13.1 de la directive n° 95/46/CE, ainsi dans le cadre d'une lutte contre le terrorisme ou le blanchiment d'argent ou pour des raisons fiscales.

(25) Van Ommeslaghe P., L'autorégulation : Rapport de synthèse, *in* L'autorégulation, Colloque Bruxelles 16 déc. 1992, Coll. Fac. Droit ULB, Bruxelles, Bruylant, p. 232. *Cf.* la définition donnée par P. Trudel, Les effets juridiques de l'autoréglementation, 19RDUS, 1988-89, n° 2, p. 251 et nos réflexions *in* Les diverses techniques de réglementation d'internet, l'autorégulation et le rôle du droit étatique, Ubiquité, n° 5, juin 2000, p. 56 et s.

(26) *Cf.* à ce propos, la typologie « *ratione personae* » proposée par Berleur J. et Ewbank T. à propos des documents d'autorégulation in Gouvernance de l'internet : Réglementation, autorégulation, corégulation ?, Gouvernance de la Société de l'Information, Cahier du CRID n° 20, Bruylant, Bruxelles, 2002, p. 34 et s.

(27) Poullet-B Havelange Y., Élaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel, janv. 97, Annexe au rapport annuel 1998 (XV D/5047/98) du groupe de travail établi par l'article 29 de la directive n° 95/46/CE, Office des publications européennes, ISBN 92-828-4305-X.

(28) Ce document est accessible à l'adresse : <www.europa.eu.int/comm/privacy>.

(29) On pourrait difficilement accepter que les règles d'entreprise ne soient pas adoptées ou en tout cas explicitement avalisées par le sommet de la hiérarchie, par exemple par le Conseil d'administration de la maison mère du groupe. Quelle valeur pourrait être accordée à la déclaration d'un simple administrateur de filiale, voire d'un président des implantations européennes du groupe, s'il n'y a pas d'une manière explicite une « couverture » de tels engagements par la maison mère ?

(30) Le fait que le détaché soit un employé d'une société du groupe n'exclut pas l'indépendance de celui-ci. Tout dépendra de la compétence et du statut de ce détaché. Sa nomination a-t-elle été justifiée par sa compétence en matière de protection des données, un veto de l'autorité de protection des données compétente pour contrôler le respect des règles était-il possible ? Pouvait-il faire l'objet d'un licenciement pour fait de sa fonction ? Rapporte-t-il directement au Conseil d'administration de la maison mère ?

(31) Document de travail n° 74, p. 12.

(32) Pour un commentaire très critique, lire Reidenberg J., *European Commission avoids Privacy disputes with the USA Privacy Laws and Bus. Int. Newsletter*, Febr. 2002, p. 9 et s.

(33) En l'occurrence, la Federal Trade Commission (FTC). Sur le rôle essentiel de cette commission dans l'économie du système de protection prévue par le « *Safe Harbor* », lire nos réflexions *in The Safe Harbor : An adequate Protection ?* Colloque international de l'IFCLA, Paris, Juin 2000, disponible sur le site du CRID <www.crid.ac.be> et celles de Reidenberg J.-R., *E-Commerce and Trans-Atlantic Privacy*, article cité, p. 740 et s. : « *The agreement is predicated on the enforcement powers of the Federal Trade Commission under section 5 of the Federal Trade Commission Act* ».

(34) Conformément aux dispositions de la Section 5 du « *Federal Trade Commission Act* » qui interdit les manœuvres et les pratiques déloyales ou frauduleuses dans le domaine du commerce ou de tout autre organisme remplissant une fonction analogue. *Cf.* la déclaration sur le site de la FTC <www.ftc.gov/ftc/mission.htm> : « *FTC enforces a variety of federal and consumer protection laws and seeks to ensure that the nations' markets function competitively and are vigorous, efficient and free of undue restrictions. The Commission also works to enhance the smooth operation of the market place by eliminating acts or practices that are unfair or deceptive* ».

(35) Notre réflexion est différente à propos des codes de conduite ou autoréglementations multilatérales dans la mesure où il est aisé de voir dans de telles formes d'autoréglementation la définition d'usages propres aux secteurs ou de règles de l'art entraînant une responsabilité aquilienne des contrevenants au code.

(36) Verbiest T. , Wery E. avec la collaboration de Salaun A. et Gobert D., Le droit de l'internet et de la société de l'information, Larcier, 2001, p. 526.

(37) *Cf.* à ce propos la décision de la Cour de cassation belge du 21 janvier 1997 (Bull. 1997, V, n° 31) où en l'espèce un employeur avait déclaré unilatéralement une augmentation de salaire et l'avait réduit par la suite.

(38) Ainsi, seule la loi allemande reconnaît légalement (§ 305 BGB) l'acte unilatéral mais exceptionnellement. L'exigence d'un contrat est la règle, qui ne subit de dérogation que dans la mesure où la loi en dispose autrement. Les auteurs français sont très réticents à une telle consécration (*Cf.* entre autres, Aubert J.-L., Encyclopédie Dalloz, Droit civil, 1987, v° Engagement unilatéral, n° 9).

(39) À cet égard les réflexions éclairantes de Coipel M., La théorie de l'engagement par volonté unilatérale et son intérêt en particulier en droit des sociétés, in Mélanges Van Ommeslaghe, 2002, p. 21 et s. L'auteur se réfère amplement à la thèse de M. Dieux X. fondée sur le principe de confiance légitime.

(40) À cet égard, Ghestin J., Le juste et l'utile dans le contrat, D 1982, chron. 1. Osman F., Avis, directives, codes de bonne conduite, recommandations, déontologie, éthique, etc. : réflexions sur la dégradation des sources privées du droit, RTD civ., 1995, p. 509 à 531 .

(41) Osman F., Avis, directives, codes de bonne conduite, recommandations, déontologie, éthique, etc. : réflexions sur la dégradation des sources privées du droit, RTD civ. 1995, p. 509 à 531. Coipel M., Quelques réflexions sur le droit et ses rapports avec d'autres régulations de la vie sociale, in Gouvernance de la société de l'information, *op. cit.*, p. 6.

(42) En particulier, la question de la prise en considération de dommages non financiers du fait du non-respect des règles n'est pas facile à résoudre. Elle constituait déjà dans le cadre des « *Safe Harbor* » un des points de discussion des plus délicats. Sur ce point, lire Reidenberg J.-R., *E-Commerce and Trans-Atlantic Privacy*, art. cité, p. 745. L'auteur conclut : « *For example, the memorandum presented by the U.S. Department of Commerce to the European Commission provides a lengthy discussion of the Privacy torts and indicates that the torts will be available. The memorandum failed to note that the applicability of these tort action has never been established by U.S. courts and is, at present, purely theoretical…* ».

(43) « *But corporate groups must bear in mind that those applying for an authorization will have to demonstrate to the grantor of the authorisation that this is effectively the case throughout the group.* » (Sur ce point et la difficulté de preuve, lire Rowe H., article cité, p. 493).

(44) Avis, p. 11.

(45) Sur la responsabilité de la filiale européenne, *supra*, n° 20.

(46) À noter que l'avis précise que c'est au groupe à démontrer le caractère suffisamment étroit des liens pour que l'on puisse en déduire l'unité de direction et l'existence d'un rapport hiérarchique et de contrôle entre le centre de décision et les membres du groupe. On rappelle que la liste des membres du groupe soumis aux règles dites contraignantes doit par ailleurs faire l'objet d'une notification. On s'interroge sur la portée que ces explications pourraient avoir en dehors du contexte de la protection de la vie privée lorsque la responsabilité du centre de décision est mise en cause pour le fait d'un membre du groupe. Il est clair que dans un tel contexte, les plaideurs pourraient tirer argument de la déclaration faite auprès de l'autorité de protection des données pour inférer l'existence d'une responsabilité du groupe (sur cette responsabilité des groupes du fait d'une filiale sous son contrôle, lire Hannoun C., *op. cit.*, n°s 150 et s., qui justifie cette responsabilité par la confiance légitime inspirée aux tiers du fait de l'existence de mécanismes internes de contrôle et de décision) ou pour appliquer certaines règles de compétence juridictionnelle, de protection des minorités, etc.

(47) Le texte de l'avis se réfère à la clause 3 qui prévoit que la personne concernée est tiers bénéficiaire des clauses contractuelles. Le mécanisme de la stipulation pour autrui pourrait expliquer dans nos droits continentaux cette exception à la relativité des contrats, principe également connu en droit anglo-saxon sous le concept de « *privity of contracts* ». On notera que le droit du tiers ne naît pas uniquement du contrat mais de la décision réglementaire de la Commission prise en vertu des compétences qui lui sont conférées par l'article 26.4 de la directive. Ainsi, les personnes concernées pourront faire valoir leur droit nonobstant l'absence de validité du contrat auquel se rattache cette stipulation.

(48) Sur une application par une multinationale des conditions requises par le Groupe de travail, lire le cas *British Petroleum* décrit par Keddle M., *How BP Makes its Global data Protection Policy a Working Reality ?* Lors du colloque « *Developing successfull Privacy relationships* » organisé par Privacy Laws and Business, 15th Annual conference, Cambridge, 1-3 juill. 2003.

(49) L'avis souligne que les principes et concepts des réglementations européennes peuvent paraître obscurs pour des personnes situées en dehors de l'Europe et dès lors doivent être traduits en langage compréhensible par elles (Avis, p. 14).

(50) Dans le cas B.P., cité note 45, l'information vis-à-vis des employés appelés à appliquer les principes du « code of practice » est réalisée via un website « *easy to use and jargon free – legal words – in order to describe data protection implications, designed for employees use and education … The website has also a section dealing with news normally describing « risks » of non compliance…The tools section intends to encourage people to "help themselves"* ».

(51) Pourquoi avoir limité aux règles juridiquement exécutoires ? Ne faut-il, pas sous réserve de secrets d'affaires, également informer à propos des mesures pratiques de contrainte ?

(52) Avis, p. 20.

(53) L'article 10 vise les informations à fournir en cas de collecte auprès de la personne concernée ; l'article 11, celles à fournir lorsque la collecte a lieu auprès d'autres sources. Ces informations s'entendent tant de l'identité du responsable que des finalités du traitement. D'autres informations peuvent être exigées mais si cela est nécessaire pour assurer un traitement loyal des données.

(54) Avis de la CPVP, p. 5.

(55) Avis, p. 16. La note 15 ajoute que le contenu de ces contrôles sera exhaustif et décrira en détail certains points particuliers.

(56) Avis, p. 16. L'avis restreint cependant le devoir de remise d'une copie à deux cas : copie automatique en cas de modification des règles notifiées, sur demande de l'autorité lorsqu'il y a coopération avec l'autorité.

(57) « *Lorsqu'on examine les formes de sanctions existantes, il est important d'établir une distinction entre les sanctions « correctives » qui imposent simplement à un responsable du traitement des données, en cas de non-respect du code, de modifier ses pratiques* ».

(58) L'avis (p. 18) précise que ces décisions auront la forme d'un acte administratif pris par l'autorité compétente et seront notifiées à la Commission européenne, voire publiées. Cette précision pose difficulté dans les pays où les autorités de protection des données n'ont pas compétence de décision comme en Belgique et où celles-ci ne pourraient dès lors être prises que par le ministre compétent.

(59) Le cas soumis à la Commission belge est à cet égard instructif. Les règles prévoyaient que l'employé dispose, en cas d'utilisation de ses données contraire aux règles de l'entreprise, d'un recours auprès d'un médiateur à l'entreprise, directeur des ressources humaines indépendant des unités de gestion. Un comité d'appel, indépendant fonctionnellement de la direction de l'entreprise, était également prévu. La Commission belge se montre satisfaite à propos de cette procédure interne de résolution de litiges « particulièrement élaborée et …

(60) Avis n° 12, p. 13.

(61) Avis n° 12, p. 14.

(62) À noter cette déclaration du Groupe 29 dans l'avis précité : « *Deux raisons justifient encore, même à supposer que le système fonctionne bien, le droit de saisir la justice (…) :*

a) l'obligation de coopération ne peut jamais garantir le respect à 100 % des règles et les personnes concernées ne sont pas nécessairement d'accord avec l'avis de l'autorité de protection des données, et

b) la compétence des autorités de protection des données (…) peut varier légèrement d'un pays à l'autre et aucune d'elles ne peut accorder de dommages et intérêts, seuls les tribunaux jouissent de cette prérogative ».

(63) Avis n° 12, p. 14.

(64) Les « *Safe Harbor Principles* », ainsi que les « *Frequent Asked Questions* » (FAQ) et la liste des entreprises ayant souscrit aux principes (plus ou moins 400 entreprises), sont publiés sur le site : <www.export.gov/safeharbor.htm>.